

Guiding SMBs Through the Cybersecurity Maze

SMB Security Survey

Telco Security Trends, H2 2024

Table of Contents

3

Introduction

5

The Quest for Effective
and Affordable SMB
Cybersecurity

6

SMBs Navigate between
Cost and Performance
Priorities

7

SMBs Are Learning to
Trust Service Providers
for Cyber Protection

8

Is Effective
Cybersecurity
Possible on an SMB
Budget?

9

Regulatory Compliance:
SMBs Are Not Prepared

10

The Allot Solution:
Easy, Effective,
Low-cost
Cybersecurity

12

Key Takeaways

13

Survey
Methodology

14

Resources

Introduction

With around half of all cyberattacks aimed at Small and Medium-sized Businesses (SMBs), these companies are at risk of anything from alienating customers to shuttering their businesses altogether. But there is hope for SMBs, with the help of Communications Service Providers (CSPs) and network-native cybersecurity solutions.

For the sake of this report, we define an SMB as a company with 50 or fewer employees. According to the MSME Forum, there are more than 300 million businesses of this size globally. Many SMBs collect and store sensitive customer data like credit card information and personally identifiable information (PII), which can be valuable to cybercriminals, making SMBs good targets for cybercrime. The likelihood of SMBs being unprepared for those crimes makes them even more attractive targets.

In this report, we discuss a recent survey of 450 SMBs worldwide, conducted in partnership with Coleman Parkes, which examined the SMBs' attitudes toward cybersecurity and the actions they are taking to mitigate cyberthreats on their businesses. Our findings revealed that SMBs are increasingly aware of their cybersecurity needs and of the benefits of network-native solutions, and they are willing to turn to CSPs for those solutions.



The opportunity for telecom providers to offer a simple, clear package of cybersecurity protections for small business and microbusiness appears significant... The value proposition for small business customers must focus on addressing threat concerns, maintaining low cost and requiring zero effort from the business."

Edward Amoroso,
CEO TAG Infosphere,
Former AT&T CISO

The Quest for Effective and Affordable SMB Cybersecurity

Numerous studies over the past few years indicate that between 40% and 50% of all cyberattacks are aimed at small businesses. In addition to more attacks, the attacks are becoming more sophisticated, making it easier for cybercriminals to deceive SMB employees into divulging sensitive data.

According to The MetLife/U.S. Chamber of Commerce SMALL BUSINESS INDEX for Q1 2024, a majority (60%) of small businesses say cybersecurity threats, including phishing, malware, and ransomware, are a top concern. They have good reason to be concerned. In our 2023 SMB SURVEY, 64% of SMBs said that they had experienced cybersecurity incidents within the previous year.

SMBs face significant challenges in raising end-user awareness of cyberthreats and teaching them how to avoid these risks. They often struggle to keep pace with emerging threats and evolving regulatory requirements. And while cyberthreats rank high as a concern for SMBs, budget constraints remain a constant concern for small businesses.

Unfortunately, many cybersecurity protection solutions, or at least the more effective ones, are costly and require either a high level of IT knowledge and expertise to manage. With limited resources, SMBs tend to seek solutions that offer strong performance without incurring substantial additional costs, which in turn limits their choices.

Fortunately, cost-effective, CSP-supplied cybersecurity solutions are available that can effectively protect SMBs. Before going into those details, let's explore insights from our recent SMB cybersecurity survey to see just how SMBs perceive and respond to cybersecurity threats.

SMBs Navigate Between Cost and Performance Priorities

When asked what the top factors were for their choice of a cybersecurity solution, 48% of SMBs prioritized performance, while 43% selected cost. Unfortunately, these two factors generally conflict with one another when it comes to cybersecurity. There are enterprise-sized solutions that require enterprise-sized budget. Then, there are consumer-level options which may fit the budget, but fall short of meeting the specific cybersecurity needs of SMBs.

Both types of solutions, as a rule, require that SMBs have a certain level of technical expertise. However, many SMBs not only face budget constraints but also lack the necessary

knowledge, and the time, to manage the daily demands of maintaining cybersecurity across all devices in their network.

What was surprising was the low relevance that SMBs put on vendor reputation, or the brand, of the cybersecurity solution that they would select. This is a positive sign for CSPs, who may not yet be strongly associated with cybersecurity excellence. It suggests that a solution meeting the key criteria of performance and cost could succeed even without an established cybersecurity brand.



SMBs are Learning to Trust Service Providers for Cyber Protection

We asked SMBs how they acquired their most recent cybersecurity solution for their businesses. More often than any other channel, SMBs answered that they turned to managed service providers (MSPs) for a solution that was part of an IT or mobile service package. In fact, SMBs chose MSPs three times more often than IT consultants, reflecting a stronger trust in service providers over other channels, including direct purchases from cybersecurity vendors.

Although service providers were the most popular channel for SMBs seeking cybersecurity solutions, only 36% of respondents reported using this channel. That is compared with a modest increase from the 26% of SMBs who relied on MSPs or CSPs in our 2023 survey¹. This indicates that while trust in service providers for cybersecurity is growing, a significant two thirds of SMBs who responded in our current survey still do not utilize CSP-provided cybersecurity services. This gap presents a substantial opportunity for CSPs in a market that is increasingly looking for affordable, effective cybersecurity solutions.

CSPs are uniquely positioned to deliver effective cybersecurity protection to SMBs. They provide connectivity to the internet, where cyberthreats lurk. This gives CSPs an advantage in which they can intercept threats within the network before they reach the end user. They are also set up to offer mass-market solutions that are zero-touch for the end user. These advantages make CSPs the ideal choice for providing comprehensive cybersecurity solutions to small and medium-sized businesses.

¹ Telco Security Trends, Q3 2023

Is Effective Cybersecurity Possible on an SMB Budget?

The amount SMBs are willing to spend on cybersecurity solutions impacts directly upon the type of protection they can implement. According to our survey, SMBs allocate an average of around \$1,400 annually for cybersecurity protection. While this budget limits their options, it does not necessarily mean they have to compromise on quality, as we will explore later in this report.

SMBs spend an avg of \$1,400/yr on cybersecurity.

When asked about their preferred way and cost of buying purchasing an IT or mobile security solution for their business, the top answer from SMBs was to have their solution bundled

with an IT package at no additional cost. This was followed closely by a preference for a bundled solution capped at 10% of total IT spend. Together, these two answers accounted for half of the SMBs surveyed, highlighting a strong demand for affordable or low-cost solutions.

Interestingly, 62% of SMBs expressed a preference for bundled services over standalone solutions, which is promising for CSPs offering cybersecurity services. While SMBs are looking for cost-effective options, their \$1,400/year budget is sufficient to cover bundled services, potentially generating incremental recurring revenue for CSPs.

The outlook becomes even more optimistic when considering that 65% of SMBs surveyed indicated that they were likely to purchase or upgrade their cybersecurity solution within the coming 12 months, with this figure rising to 73% in the UK. Combine this with a full 92% of SMBs who report having at least a basic understanding of the benefits of network-based security solutions. This indicates a market that is not only increasingly aware about CSP-offered cybersecurity services but is also ready to invest in them in the near future.



Regulatory Compliance: SMBs Are Not Prepared

In the digital era, regulatory compliance is a significant driver for cybersecurity initiatives across industries. Small and medium-sized businesses face a wide range of regulatory requirements designed to protect sensitive information and ensure data privacy. Failing to meet these standards can result in severe penalties, legal repercussions, and a loss of customer trust. Key regulations include the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). For more information on the regulatory requirements that SMBs need to comply with, see the short report, ['Navigating Regulatory Requirements: Why Cybersecurity is Crucial for Small and Medium Businesses.'](#)

Our survey reveals that SMBs are grossly underprepared and at risk of non-compliance with basic cybersecurity practices mandated by law. These practices include implementing cyber protection services if the SMB accepts digital payments, collects personal data on end-users, or works with certain key federal bodies. This lack of preparedness exposes SMBs to a host of compliance risks, fines and potential disruptions impacting their business continuity. With that in mind, only 1 in 3 SMBs claim to be fully prepared for changes in cybersecurity regulations impacting their

business, and just 24% have hired compliance experts. This leads to gaps in awareness and the ability to adequately protect themselves.

While no single cybersecurity solution can fully address all the regulatory compliance needs of an SMB, a network-native cybersecurity solution provided by a CSP can help mitigate a significant portion of these concerns.



The Allot Solution: Easy, Effective, Low-cost Cybersecurity



Allot offers CSPs a zero-touch, network-native solution that they can offer as a service to SMBs, particularly those with limited resources and expertise to manage their own tech support. This network-native solution is implemented directly within the CSP's network. This means that it not only effectively intercepts cyberthreats before they reach the end user's device; It also eliminates the need for end users to install or update any software to enjoy the protection of the network-native solution.

SMBs need a robust, automated cybersecurity solution that secures their business without requiring technical skills for deployment and maintenance. Moreover, SMBs want cybersecurity protection solutions that are budget-friendly. Priced at \$10 to \$20 dollars per month, the network-native solution from Allot is an ideal fit for SMBs.

For the CSP, a zero-touch, network-native cybersecurity solution not only boosts ARPU/ARPA but also enhances brand loyalty. SMBs will increasingly see their CSPs not just as utility providers but rather as integrated business partners who safeguard their operations from Cyberthreats.



This product (Allot Conexion Segura) exceeded our expectations... We were surprised by the response, because what we had planned to achieve in 4 years, we already reached in 9 months."

Victor Deutsch
Former Head of Cybersecurity
Product Line, Telefónica SMB Spain

Key Takeaways

SMBs are greater targets for cyber crime than ever before. They are concerned with budget and performance of solutions aimed at protecting their businesses, and they are ready to purchase cybersecurity solutions from CSPs.

**SMBs need
cybersecurity
solutions**

**Simplicity and
cost are key**

**CSPs are
strategically
positioned to
help**

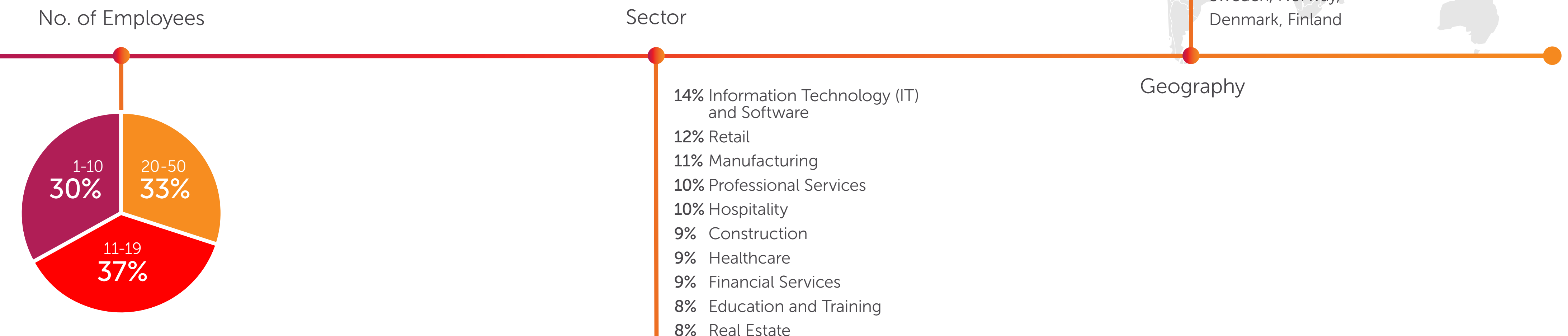
**SMBs are likely
to purchase/
upgrade
cybersecurity
solution within
12 months**

**SMBs are not
prepared for
regulatory
changes**

Survey Methodology

During July of 2024, Coleman Parkes Research set out to gain insights into SMB perspectives on cybersecurity and to discover how they protect their businesses against cyberthreats.

The survey included 450 SMB technology decision-makers from the United States, Canada, the UK, Germany, Sweden, Norway, Denmark, Finland and the Philippines. These participants were surveyed online about the current state of their cybersecurity, their willingness to invest in cybersecurity solutions, and their views on cybersecurity offerings from CSPs.



Resources

The following resources provide additional insight to CSPs looking to secure their SMB subscribers.



Webinar – How CSPs Can Monetize the Cybersecurity Maze for SMBs

[Watch Now](#)



Navigating Regulatory Requirements: Why Cybersecurity is Crucial for Small and Medium Businesses

[Learn more](#)



Network Security for Business Customers

[Learn more](#)



SMB Cybersecurity Protection Report 2024

[Read Report](#)



SMBs Need an Air Bubble in the Sea of Cyber Threats

[Read Blog](#)



Don't Miss the Growing SMB Security Services Opportunity

[Read Report](#)

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and converged security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-native security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry-leading network-native security-as-a-service solution is already used by many millions of subscribers globally.

To learn how CSPs can protect their business subscribers, visit

www.allot.com »



© 2024 Allot Ltd. All rights reserved. Specifications subject to change without notice. Allot and the Allot logo are registered trademarks of Allot. All other brand or product names are trademarks of their respective holders.



www.allot.com

Sep 2024